Kiedy ciąg jest losowy?

Szymon Draga

Szczyrk, 27 listopada 2010r.

Definicja 1. *Maszyną Turinga nazywamy czwórkę uporządkowaną*

$$(Q, \Sigma, \delta, q_0),$$

gdzie Q jest (skończonym) zbiorem stanów,
Σ (skończonym) alfabetem taśmy,
$\delta\colon Q \times \Sigma \to Q \times \Sigma \times \{L, R\}$ funkcją przejścia, która może być częściowa,
$q_0 \in Q$ stanem początkowym.

W dalszym ciągu zakładamy, że $\Sigma = \{0, 1, \#\}$, a $\#$ interpretujemy jako znak spacji. Ponadto, L oznacza ruch w lewo, zaś R w prawo.

Przykład 1. $M = (\{q_0\}, \{0, 1, \#\}, \delta, q_0)$, gdzie $\delta(q_0, i) = (q_0, 1 - i, R)$ dla $i = 0, 1$, jest maszyną Turinga, która zamienia zera na jedynki, i na odwrót.

Definicja 2. *Niech $M = (Q, \Sigma, \delta, q_1)$, gdzie $Q = \{q_1, \ldots, q_n\}$, $\Sigma = \{\sigma_1, \sigma_2, \sigma_3\}$ ($\sigma_1 = 0,\ \sigma_2 = 1,\ \sigma_3 = \#$) oraz $(L, R) = (d_1, d_2)$. Kodem maszyny M nazywamy najkrótszy z ciągów, będących konkatenacją 0^n i wszystkich przejść funkcji δ zakodowanych jako*

$$10^i 10^j 10^k 10^l 10^m,$$

gdy $\delta(q_i, \sigma_j) = (q_k, \sigma_l, d_m)$.

Uwaga: Najkrótszy ciąg to ciąg o najmniejszej długości spośród wszystkich ciągów opisujących daną maszynę (w szczególności, ich długości zależą od numeracji stanów). Należy zatem wybrać najkrótszy ciąg po uwzględnieniu wszystkich możliwych zmian numeracji.

Przykład 2. Maszynę z przykładu 1 kodujemy jako

$$0\,101010100100\,101001010100.$$

Definicja 3. *Niech M będzie maszyną Turinga. Oznaczmy przez $M(y)$ ciąg, który jest wynikiem działania maszyny M, jeśli na wejściu podaliśmy ciąg y. Złożonością Kołmogorowa ciągu x na maszynie M nazywamy liczbę*

$$K_M(x) = \min\{|y| \colon M(y) = x\}.$$

Intuicyjnie, złożoność Kołmogorowa (przy ustalnonej maszynie Turinga) mierzy stopień skomplikowania ciągu.

Przykład 3. Złożonością Kołmogorowa dowolnego ciągu binarnego na maszynie Turinga z przykładu 1 jest jego długość.

Przykład 4. Niech M będzie maszyną Turinga podwajającą każdy znak oraz niech $x = (x_1, \ldots, x_n)$. Wtedy

$$K_M(x) = \begin{cases} \frac{n}{2}, & \text{gdy n jest parzyste i } x_{2i-1} = x_{2i} \ (i = 1, \ldots, \frac{n}{2}) \\ \infty & \text{w przeciwnym przapadku.} \end{cases}$$

Definicja 4. *Maszynę Turinga U nazywamy asymptotycznie optymalną, jeżeli dla każdej maszyny Turinga M, istnieje taka stała $c \in \mathbb{R}$, że dla każdego ciągu x zachodzi nierówność*

$$K_U(x) \leqslant K_M(x) + c.$$

Kwestię istnienia asymptotycznie optymalnej maszyny Turinga rozstrzyga następujące twierdzenie:

Twierdzenie 1. Istnieje asymptotycznie optymalna maszyna Turinga.

Dowód. Niech U będzie dowolną uniwersalną maszyną Turinga tzn. maszyną symulującą działanie dowolnej maszyny. Można wykazać, że maszyna taka istnieje. Sposób wprowadzenia ciągu do takiej maszyny, aby zainicjować działanie innej maszyny na ciągu x, może być następujący:
Podwajamy każdy znak w kodzie maszyny, którą chcemy symulować, konkantenujemy otrzymany w ten sposób ciąg z 01 i ciągiem x. Łatwo zauważyć, że z tak otrzymanego ciągu można jednoznacznie odtworzyć symulowaną maszynę i ciąg x.

Pokażemy, że maszyna U jest asymptotycznie optymalna. W tym celu ustalmy maszynę Turinga M i oznaczmy jej kod przez m. Zauważmy, że przy powyższym sposobie kodowania mamy

$$K_U(x) \leqslant 2 \cdot |m| + 2 + K_M(x)$$

dla dowolnego ciągu x. Oznacza to, że w definicji 4 możemy przyjąć $c = 2 \cdot |m| + 2$, czyli maszyna U jest asymptotycznie optymalna. □

Definicja 5. *Złożnością Kołmogorowa ciągu x nazywamy jego złożność Kołmogorowa na dowolnej, lecz ustalonej, aymptotycznie optymalnej maszynie Turinga i oznaczamy $K(x)$.*

Uwaga: Złożność Kołmogorowa ciągu zależy od wyboru asymptotycznie optymalnej maszyny Turinga, jednak, jak łatwo sprawdzić, dla pewnej stałej złożoność dowolnego ciągu na dwóch różnych maszynach asymptotycznie optymalnych różni się co najwyżej o tę stałą. W związku z tym uzasadnione jest przyjęcie następującej definicji:

Definicja 6. *Ciąg $(c_n)_{n=1}^{\infty}$, gdzie $c_n = 0, 1$ dla $n \in \mathbb{N}$, nazywamy losowym, jeżeli*

$$\lim_{N \to \infty} \frac{K((c_n)_{n=1}^{N})}{N} = 1.$$

Przykład 5. Ciąg $(x_n)_{n=1}^{\infty}$, w którym każdy znak jest podwojony nie jest losowy. Istotnie, niech M będzie maszyną Turinga podwajającą każdy znak oprócz pierwszego, jeśli pierwszym znakiem jest 0, oraz podwajającą każdy znak oprócz pierwszego i ostatniego w przeciwnym przypadku (pierwszy znak jest zamieniany na #). Wówczas

$$\limsup_{N\to\infty} \frac{K((x_n)_{n=1}^{N})}{N} \leqslant \lim_{N\to\infty} \frac{K_M((x_n)_{n=1}^{N})}{N} = \frac{1}{2}.$$

Literatura

[1] Grzegorz Gutowski
Dowód pierwszego twierdzenia Gödela o niezupełności arytmetyki oparty o złożoność Kołmogorowa
http://www.logic.amu.edu.pl/images/2/26/Gutowskikolmogorow.pdf